Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/IS04/000007

International filing date: 12 July 2004 (12.07.2004)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/485,733
Filing date: 10 July 2003 (10.07.2003)

Date of receipt at the International Bureau: 06 September 2004 (06.09.2004)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

1211159

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

August 12, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: *60/485,733*
FILING DATE: *July 10, 2003*

Certified by

Jon W Dudas

Acting Under Secretary of Commerce
for Intellectual Property
and Acting Director of the U.S.
Patent and Trademark Office

MS PROVISIONAL PATENT APPLICATION
PTO/SB/16(8-00)

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 C.F.R. § 1.53 (c).

Filing Date	July 10, 2003	Docket No.	3535-0123P

INVENTOR(s)/APPLICANT(s)

Given Name (first and middle [if any])	Last Name	RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)
Steindor S. Stefan	GUDMUNDSSON HRAFNKELSSON	Reykjavik, Iceland Reykjavik, Iceland

☐ Additional inventors are being named on the separately numbered sheets attached hereto

TITLE OF THE INVENTION (280 characters max)

SECURE AND AUDITABLE ON-LINE SYSTEM

CORRESPONDENCE ADDRESS

Birch, Stewart, Kolasch & Birch, LLP or Customer No. 2292
P.O. Box 747
Falls Church

STATE	VA	ZIP CODE	22040-0747	COUNTRY	U.S.A.

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification *Number of Pages:* 19
☒ Drawing(s) *Number of Sheets:* 4
☐ Application Data Sheet. See 37 CFR 1.76.
☐ Other (specify):_____

METHOD OF PAYMENT *(check one)*	PROVISIONAL FILING FEE
☒ Applicant claims small entity status. See 37 CFR 1.27.	☒ Small Entity ($80.00)
☒ A check or money order is enclosed to cover the Provisional filing fees.	☐ Large Entity ($160.00)
☒ The Commissioner is hereby authorized to charge filing fees and credit Deposit Account Number 02-2448, if necessary.	

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

Date: July 10, 2003

By _____
Joe McKinney Muncy, #32,334

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

KM/asc
3535-0123P

(Rev. 06/02/03)

SECURE AND AUDITABLE ON-LINE SYSTEM

FIELD OF INVENTION

The present invention relates to generation of security and audit ability in an on-line system, such as an instant ticket lottery, a code generation system, an encryption system, or a money transfer system. More particularly, the present invention relates to secure management of an on-line system, in particular an on-line ticket lottery.

BACKGROUND OF THE INVENTION

Modern communication networks such as the Internet, Wide Area Networks (WANs) and Local Area Networks (LANs), have proven to be enormously efficient means of organizing and distributing digital data. This has resulted in a widespread use of these networks for business, entertainment and personal applications. The Internet is now a common network for performing electronic commerce, banking and electronic mail transactions as well as being widely used for academic purposes, providing information and gaming and betting activities.

The traditional gaming and betting systems have been based on direct interaction in a common physical location, such as casinos, bingo halls, and sports betting halls and buying physical lottery tickets. The Internet, however, offers a solution for those who cannot visit the physical locations for some reason, such as hospitalised individuals, or people with impaired mobility due to a handicap, or for people living in remote areas far away from traditional gaming and betting facilities.

Ticket lottery games are popular sources of revenue for governmental bodies and step is performed at charitable organizations, being either a scratch-off or pull-tab game with a number of pre-printed tickets. A lottery ticket comprises a printed result indicator, indicating whether or not a particular ticket is a winning ticket and, if so, the nature of the winning. Several electronic lottery games have been implemented through computer-based systems. US 5,324,035 incorporates all information required to define a game play into a video lottery system, including data for various graphic symbols to be displayed to the player through the player terminal. This arrangement results in relatively large amounts of data having to be transferred to the player terminal for each game play.

US 4,494,197 discloses a method for wagering, which utilizes a counter register and winning ticket table situated in a central processor unit. Upon a request from a player terminal, the value in the counter register is incremented and then the winning ticket table is queried to determine if the resulting count corresponds to a winning electronic ticket. The central processor then sends back to the player terminal a packet of information including a winning or losing code as appropriate. The winning code includes the amount won on the play.

US 4,842,278 describes the interconnection of two or more state lottery games into a national game. This lottery is a betting game wherein the winning odds are calculated based upon an input from the player throughout the entire region, and not just from a single state. Payoffs are provided according to a total amount wagered and the number of winning bettors, somewhat like a pari-mutuel system.

US 5,158,293 describes another multiple level game, in the sense that players may be sequentially eligible for different prizes or payoffs during the course of play. However, this document makes no mention of any different wagering denominations by different groups of bettors, and resulting different pools and accordingly different prizes or payoffs. In US 6,017,032 is disclosed a lottery game and method of play, in which provision is made for wagers at different denominational levels. Each wager of a given denominational level is placed in a sep step is performed at a rate jackpot pool, with the winner or winners paid from that pool. All wagers of all denominations pass through a central controller or agency, where they are distributed to the appropriate pool or pool fraction or portion.

The use of true random number generators (TRNG), to deliver so called true or non-deterministic random numbers are well known *per se* in the art. Such devices use a low-frequency oscillator and a high-frequency oscillator, and are, e.g., disclosed in US 4,641,102; US 5,781,458 and US 6,061,702. In another document, methods of generating true random numbers using components normally available on personal computers, is described (US 2003037079). The method includes generating true random number sequences of calculable entropy content. The entropy is derived from a random noise component, or transition jitter, in one or both of a low- and a high-frequency signal source that are coupled to a processor for producing the random numbers. The high-frequency signal source includes a frequency multiplier that significantly increases the size of the noise component in the high-frequency signal. This will allow for rapid production of true random numbers of known, high quality.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide an on-line system, which may be managed in a secure manner.

It is a further object of the present invention to provide an on-line system, which is sufficiently secure to meet the demands of, e.g., instant ticket lotteries.

It is an even further object of the present invention to provide an on-line system having limited access in order to obtain a secure and controllable management of the system.

It is an even further object of the present invention to provide a method for managing such an on-line system in a secure manner.

It is an even further object of the present invention to provide a method for managing such an on-line system in a controllable manner.

It is an even further object of the present invention to provide a device for managing such an on-line system in a secure manner.

It is an even further object of the present invention to provide a device for managing such an on-line system in a controllable manner.

According to a first aspect of the present invention the above and other objects are obtained by providing a method of obtaining security and audit ability in an on-line system, the method comprising the steps of:

- generating a random number by means of a random number generator,
- providing a sequence number for each of the random numbers generated so as to create a random number - sequence number pair,
- storing the created random number - sequence number pair in a storage means,

the method further comprising the step of, at a chosen time, verifying stored random number - sequence number pairs, so as to ensure that every stored random number - sequence number pair is an authentic random number - sequence number pair.

According to a second aspect of the present invention the above and other objects are obtained by providing a secure and auditable on-line system comprising:

- a random number generator,
- means for providing a sequence number for each generated random number, so as to create a random number - sequence number pair,
- storage means for storing the created random number - sequence number pair,
- verifying means for verifying, at a chosen time, stored random number - sequence number pairs, so as to ensure that every stored random number - sequence number pair is an authentic random number - sequence number pair.

An important feature of the present invention is the audit ability, a mechanism that verifies all random number - sequence number pairs generated by the system. The random number -sequence number pairs stored in the storage means are the basis for the audit process, wherein a routine check can be made at a chosen time. By double-checking the pairs the auditors can spot if an intruder is bypassing the random number generator in order to select especially favourable sequence numbers.

In the present context the term "security" refers to techniques for ensuring that data stored in the storage means cannot be unrightfully read or tampered with in any way, such as selecting only certain data from a processing means or storage means, which are to be sequentially or randomly distributed.

In the present context the term "audit ability" refers to the ability to maintain a record for a system showing if the system has been invaded or illegally accessed and what operations were performed during a given period of time. The audit process may be set up in a way that a special audit trail means enables the administrators to monitor use of network system.

In the present context the term "on-line" refers to a communication network, such as, but not limited to the Internet, Wide Area Networks (WANs) and Local Area Networks (LANs). Further more the term "on-line" refers to any network comprising a gaming platform and a plurality of end user clients.

In the present context the term "sequence number" refers to any number being selected from an array of numbers comprising a certain amount of numbers, which have been evenly and sequentially lined up. The numbers may be selected from the group of, but not limited to 10, 100, 1.000, 10.000, 100.000, 1.000.000, 10.000.000 or 100.000.000 numbers between any two number such as, but not limited to 0 and 1.

In the present context the term "verify" refers to a process, where actions or transactions in a system are checked. The term may further refer to presence or absence of data in a system and, if the date is present, then the verifying step may refer to whether the data have been manipulated or not. The verification may be a manual or automatic process performed routinely or randomly. A random number - sequence number pair is "authentic" if the verifying step establishes that it was rightfully created and stored by the system, i.e. it has not been tampered with, and it was not stored by a party which is not entitled to create and store random number - sequence number pairs.

The storage means for storing the random number - sequence number pairs is preferably an electronic storage means, such as a hard disc drive, a CD-ROM, a DVD disc, a floppy disc, a magnetic tape, or any other suitable kind of data storage means.

The verifying step may be performed at at least substantially equal time intervals, such as once or twice every day, every second day, every week, every month, every hour, etc. In this embodiment the verifying step is performed as a routine action, where all stored random number - sequence number pairs are verified as a precaution. However, it may

further be possible to perform the verifying step at a chosen time not falling within the normal time for a routine action. This may, e.g., be desirable in case there is reason to believe that some of the numbers have been tampered with, or that somebody has unrightfully gained access to the stored numbers.

In a preferred embodiment the generated random number is a true random number, and the random number generator is a true random number generator. In the present context the term "true random number generator" refers to a device that generates true random numbers, typically by sampling and processing a *source of entropy* outside the device. The entropy source can, e.g., be a radioactive source, atmospheric noise from a radio or lava lamps.

The storing step may be performed by storing the random number - sequence number pair in a storage means with limited access. The term "limited access" may be interpreted as meaning that only certain persons have access to the storage means. It may, e.g., be a secure enclosed system; a so-called "black box" and/or it may comprise a locked compartment.

Furthermore, the random number generator may have limited access. The storage means and the random number generator may be positioned in the same limited access area (e.g. the same "black box" or the same locked compartment) of the system. The limited access area may further comprise a sequence number generator, so that the generation of the random number, the generation of the sequence number, and the storing of the random number - sequence number pair all take place within the limited access area, thereby reducing the risk that any of the numbers may be tampered with, or that a false/unauthentic random number - sequence number pair may be stored in the storage means.

Access to the limited access area(s) may be obtained only by one or more authorised persons, such as by two or more authorised persons. Each of the two or more authorized persons may represent an authority, so that at least two authorities are represented when access to the limited access area(s) is obtained. At least one of the authorised persons may represent an operator, and at least one of the authorised persons may represent an auditor. In this embodiment, at least one person representing the operator, and at least one person representing some kind of auditing authority have to be present in order to gain access to the limited access area(s). The person representing the operator may be a person pointed out by or employed by the entity, which administers the on-line system for management and supervision of the system. The person representing the auditor may be a government official person supervising the operation of the on-line system, e.g. in order

to ensure that the system fulfils certain official requirements, e.g. in order to maintain public trust in the system.

In a preferred embodiment of the present invention the security and audit ability are obtained by a closed system, wherein the secure and close system may be a so-called "black box" unit. The "black box" may comprise the following components:

- A locked box,
- A random number generator,
- A sequence number generator, and
- Storage means

The "black box" can further be described as an environment hosting data storage means, processors and generators and the "black box" may provide a physical barrier which only authorized administrators and auditors have access to.

The method may further comprise the step of issuing a ticket comprising information relating to the sequence number. This information may be the sequence number itself. The ticket may be a token or a receipt to a user of the on-line system, and the ticket may indicate the actions performed by the system on request from the user, such as the generation of a code or an encryption or decryption key, a money transaction, or the generation of a lottery ticket. Preferably, the ticket does not comprise the generated random number. However, it may comprise information relating to the random number. Thus, in case the on-line system is a ticket lottery, the random number determines whether or not the ticket is a winning ticket, and such information may advantageously be present on the ticket. For some purposes, however, the ticket may comprise the actual random number.

In a preferred embodiment the on-line system is a lottery, and the issued ticket is a lottery ticket. In this case the ticket may further comprise information relating to a winning/no-winning category of the ticket. As mentioned above, this information may relate to the generated random number.

In case the on-line system is a lottery, the step of issuing a ticket may be based upon the random number and a probability table, in which case the method may further comprise the step of updating the probability table in response to the issued ticket, so as to maintain an at least substantially fixed winning/no winning ratio. Thus, the on-line ticket lottery functions as if it was a conventional ticket lottery in which all the tickets have been created in advance. But in the on-line ticket lottery according to the present invention the

tickets have not been created in advance, but are created when they are drawn, i.e. when a user requests a ticket.

In one embodiment of the present invention the on-line system is a code generation system. According to this embodiment the random number - sequence number pair represents a code for the protection of ID numbers or social security numbers in a database. The database may contain personal information on individuals such as, but not limited to health records, financial records or social records.

In another embodiment of the present invention the on-line system is an encryption system. According to this embodiment the random number - sequence number pair represents an encryption and/or a decryption key. It is a great advantage that such keys may be created, stored and used in a secure and auditable manner, since this increases the trust that the public may have in the system.

In yet another embodiment of the present invention the on-line system is a money transfer system. It may be a cash point or a system to electronically transfer money from one account to another. In this case it is ensured by the verifying step that only the right persons transfer/withdraw money from a specific account.

The method may further comprise the step of alerting an operator in case the verifying step results in the discovery of one or more non-authentic random number - sequence number pairs. The alert may be in the form of a printed report indicating that something is wrong, and that appropriate actions should therefore be taken. Alternatively or additionally, the alert may be in the form of an electronic message, e.g. an e-mail sent to an operator, or an electronic flag, or any other suitable kind of alert.

The step of generating a random number may be performed upon the request from a user. Thus, a lottery ticket, a code, an encryption/decryption key, a money transfer, etc. is created/performed on the request of a user. The user thereby initiates the operating steps of the present invention.

The method may further comprise the step of receiving payment from a user. This is particularly useful in case the on-line system is a system offering services, which the user should pay for, e.g., a ticket lottery, a code generation system or an encryption system. Preferably, the step of receiving payment is performed before the random number is generated, thereby enabling the system to make sure that appropriate payment for the service has been received before the service is provided. The payment step may, e.g., be performed by the user delivering bank notes or coins to a paying machine. Alternatively or

additionally, the payment step may be performed by means of a card reader for credit cards or cash cards (smart cards). Alternatively or additionally, the payment step may be performed by means of an electronic money transfer, e.g. an account-to-account transfer, or a transfer from an electronic wallet to an account.

The verifying step may comprise checking that a certain number of random numbers has been generated. This is particularly useful when the on-line system is a ticket lottery. In this case the certain number of random numbers corresponds to the number of possible lottery tickets in the game. When all the tickets have been drawn, the game should, of course, be closed.

The verifying step may comprise the steps of:

- checking whether a given random number - sequence number pair has previously been stored in the storage means,
- marking said given random number - sequence number pair as a true pair in case it has previously been stored in the storage means, and
- alerting an operator in case the given random number - sequence number pair has not previously been stored in the storage means.

In this embodiment it is assumed that only authentic random number - sequence number pairs have been stored in the storage means, and that all authentic random number - sequence number pairs have been stored.

According to a thied aspect of the present invention the above and other objects are obtained by providing a device for obtaining security and audit ability in an on-line system, the device comprising:

- a random number generator,
- means for providing a sequence number for each generated random number, so as to create a random number - sequence number pair,
- storage means for storing the created random number - sequence number pair,
- verifying means for verifying, at a chosen time, stored random number - sequence number pairs, so as to ensure that every stored random number - sequence number pair is an authentic random number - sequence number pair,

the verifying means further comprising:

- means for checking whether a given random number - sequence number pair has previously been stored in the storage means,

- means for marking said given random number - sequence number pair as a true pair in case it has previously been stored in the storage means, and
- means for alerting an operator in case the given random number - sequence number pair has not previously been stored in the storage means,

wherein the storage means and the random number generator have limited access.

EXAMPLES

Example 1

Generation of security in an on-line ticket lottery

Objectives

To reach audit ability a in an on-line ticket lottery by attachment of a secure closed system (a so-called "black box"), providing physical security for services relating to creation of the tickets. The "black box" service that is locked and can only be opened while "auditors" are present. The "black box" will offer services that can be audited.

Methods

The Audit Process (AP) is based on audit ability, and is reached by attaching a "True Random Number Generator" to a PC compatible machine in a locked box generating a true random number and a sequence number. Every time the Gaming Platform (GP) gets a request from a player it requests a true random number from the "black box". A random number - sequence number pair is created, sent to the GP and saved in the "black box". The audit process goes through every instant record in the GP database and compares the random number - sequence number pair to the contents of the "black box".

Results

The audit ability of the system is reached by attaching a "True Random Number Generator" to a PC compatible machine in a locked box that offers two services:

- Auditable True Random Number by use of a sequence number
- Approving the specific TRN for a specific winning category

To reach audit ability the "black box" will return sequence number together with each random number. This sequence number will be saved with the ticket. The Approving

service can then be used later to approve that the specific ticket (winning ticket) actually got a random number that resulted in a winning.

Example 2

Generation of audit ability in an instant ticket lottery

Objectives

To strengthen security of an on-line ticket lottery, a process has been defined that will periodically approve sold Instant Tickets according to rules specified by the lottery. The security system should be a flexible process that can be run periodically and approve a batch of tickets according the secure services of a "black box".

Methods

Upon a request from the Gaming Platform (GP), a random number - sequence number pair is created and saved in the "black box". A routine mechanism will start at predetermined times like once or twice every day. If the system is being manipulated by an intruder, the system will alert the administrators of the lottery. The Audit Process (AP) verifies the random number - sequence number pairs saved in a storage means also exists in the "black box" and an alert is given if something does not match, like if there are gaps in the sequence in the GP database. The AP also recalculates each instant ticket drawn from the pool and verifies that it is according to the random number drawn. The security system can also aid in pool management of the lottery by sending messages to the GP that all the tickets in a pool have been sold and all the random number - sequence number pairs are confirmed.

Results

One of the functions of the security mechanism is to double check at all times the correctness of the winning selection according to Lottery's pre-specified rules as well as approving that the SecureTRNG is not generating more random numbers than are used by the Instant Ticket Service. That could be the case if intruders will invade the system to get a supposed to be good "random" number and only buy tickets when he gets one. Lottery can specify the period (usually daily) and the prize categories that are checked. A default setting orders checking of all but lowest price and no winning tickets. This will allow the system to make sure that winning tickets, possibly generated by bypassing the Secure-TRNG, are spotted by the end of the day. Another function is comparison of all sequence numbers in the database against of all sequence numbers serviced by the "black box" to avoid the possibility that a process can ask for a random number - sequence number pair

without paying for the ticket or only pay if the random has probability of winning higher than even distribution.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described in more detail by means of the accompanying drawings in which:

Fig. 1 shows a block diagram describing how speed is generated in an on-line system according to the present invention,

Fig. 2 shows a block diagram describing the overall audit process of an on-line system according to the present invention,

Fig. 3 shows the features of the audit process of Fig. 2, and

Fig. 4 shows a manual take over process of an on-line system according to the present invention

DETAILED DESCRIPTION OF THE DRAWINGS

Fig. 1 describes the method of generating speed in a ticket lottery and how one or several pools are managed during a lottery game. The process of the method is initiated by a request from a customer. The customer accesses an instant lottery game through the Internet, by placing an electronic request using, e.g., a PC compatible client or an embedded POS Lottery device. The request is directed to the Gaming Platform (GP), comprising a processing means including a probability table and storage means. The probability table represents the current game and resembles unsold tickets in all existing pools of the game. The GP handles the request by charging the customer for the ticket and when the GP has received a confirmation that a payment has been made the GP requests a true random number (TRN). Based on the current instant pool (i.e. the probability table) and the random number, the GP calculates the category the ticket belongs to. The instant pool is changed after generation of each ticket according to the category (one less in that particular category), by updating the probability table. The game transaction, including a sequence number and the category to which the ticket belongs to, is saved by the GP. The platform is thereafter ready to service the next customer.

Based on criteria set by the Lottery, a minimal number of tickets in the lottery or in each category are allowed. If these criteria are not met, a new pool or category may be added into the lottery. If a new pool or category is added into the lottery, the probability table is updated, and the platform is thereafter ready to service the next customer.

Fig. 2 describes the overall audit process offered by the system. The process is initiated by selecting a sequence range, which covers all sequence numbers issued from the last time of auditing and to the time of present auditing. The process verifies each pair stored in a "black box" of the system and compares them to all pairs stored in the Gaming Platform (GP). This process is described in detail in Fig. 3. If the pair is confirmed the GP marks the pair as confirmed and starts verifying the next pair, provided that there are more pairs stored in the GP. However, if the pair is not confirmed a report is printed alerting the administrators/auditors, and appropriate actions are taken. This basically results in manual take over (described in Fig. 4).

If there are no more pairs in the GP, the audit process gets unconfirmed pairs, a process described in more detail in Fig. 3. If there are no unconfirmed pairs in the system the audit process asks if a certain pool should be closed. Based on the current status of the pool, e.g. if all the tickets in the pool have been sold, the pool is closed. If unconfirmed pairs exist in the "black box", but not in the GP, the audit process prints a report alerting the administrators/auditors and appropriate actions are taken.

Fig. 3 describes the features 1-3 of the audit process provided by a secure closed compartment, a so-called "black box", comprising processing means, a true random number generator (TRNG) and storage means.

The first feature 1 of the "black box" provides a true random number (TRN) to the Gaming Platform (GP) each time the GP receives a request from a customer. For each TRN generated, a sequence number is generated from the processing means. By attaching the two numbers to each other a true random number - sequence number pair is created. The true random number - sequence number pair is saved in the "black box", in order to reach audit ability, and then returned to the GP. The audit process goes through every instant record in the GP database and compares the true random number - sequence number pair to the contents of the "black box".

The second feature 2 is the confirmation of the true random number - sequence number pairs. The pairs stored in the GP are compared to the pairs stored in the "black box". If the pair is confirmed, the pair is returned and marked as a true pair and the process continues until all pairs have been verified. If the pair is not confirmed for any reason, the system prints a report alerting the administrators/auditors and appropriate actions are taken. When a pair is returned it is necessary to calculate the winning category specified on the ticket in order to confirm that it is in accordance with the information presented on the ticket. This is done by re-building the probability table, in a similar way it was done when the ticket was created.

The third feature 3 of the black box allows the audit process to ask for unconfirmed pairs in the black box over a period that has already been confirmed (by use of the second feature (Compare pairs)).. If unconfirmed pairs remain in the system after the audit

process has been performed, the system prints a report alerting the administrators/auditors, and appropriate actions are taken.

Fig. 4 describes the manual take over process, which is initiated if an alert is sent to the auditors and administrators due to unconfirmed pairs in the system.
If there are extra pair(s) in the BW Solutions the auditors need to analyse matters such as, but not limited to:

- Have new versions of Betware Solutions been deployed?
- Have the administrators accessed the system during the period that is being audited, and if so what were their actions
- The journal logs can be viewed in order to verify that the original records have not been tampered with or changed manually
- Have hackers accessed the system during the period being audited and if so what were their actions

If there are extra pairs in the "black box", the auditors need to analyse matters such as, but not limited to:

- Have new versions of Betware Solutions been deployed?
- Have hackers accessed the system during the period being audited and if so what were their actions?
- Analyse who has access to get service of the "black box"
- Are pairs missing due to failure in the processes that have confirmed new random number - sequence number pairs, but did not finish the transactions? (can be normal if two phase commit is not supported between BW Solutions and the "black box").

Based on what the auditors, and security experts if needed, may find to be the reason for the alert, necessary arrangements need to be made. These may involve alerting authorities or solving internal problems.

CLAIMS

1. A method of obtaining security and audit ability in an on-line system, the method comprising the steps of:

- generating a random number by means of a random number generator,
- providing a sequence number for each of the random numbers generated so as to create a random number - sequence number pair,
- storing the created random number - sequence number pair in a storage means,

the method further comprising the step of, at a chosen time, verifying stored random number - sequence number pairs, so as to ensure that every stored random number - sequence number pair is an authentic random number - sequence number pair.

2. A method according to claim 1, wherein the verifying step is performed at at least substantially equal time intervals.

3. A method according to claim 1 or 2, wherein the generated random number is a true random number, the random number generator being a true random number generator.

4. A method according to any of claims 1-3, wherein the storing step is performed by storing the random number - sequence number pair in a storage means with limited access.

5. A method according to any of claims 1-4, wherein the random number generator has limited access.

6. A method according to claim 4 or 5, wherein access to the limited access area(s) can only be obtained by one or more authorised persons.

7. A method according to claim 6, wherein access to the limited access area(s) can only be obtained by two or more authorised persons.

8. A method according to claim 7, wherein the two or more authorised persons each represents an authority, so that at least two authorities are represented when access to the limited access area(s) is obtained.

9. A method according to claim 8, wherein at least one of the authorised persons represents an operator, and at least one of the authorised persons represents an auditor.

10. A method according to any of claims 1-9, further comprising the step of issuing a ticket comprising information relating to the sequence number.

11. A method according to claim 10, wherein the on-line system is a lottery, and the issued ticket is a lottery ticket.

12. A method according to claim 11, wherein the ticket further comprises information relating to a winning/no winning category of the ticket.

13. A method according to claim 11 or 12, wherein the step of issuing a ticket is based upon the random number and a probability table, the method further comprising the step of updating the probability table in response to the issued ticket, so as to maintain an at least substantially fixed winning/no winning ratio.

14. A method according to any of claims 1-10, wherein the on-line system is a code generation system.

15. A method according to any of claims 1-10, wherein the on-line system is an encryption system.

16. A method according to any of claims 1-10, wherein the on-line system is a money transfer system.

17. A method according to any of claims 1-16, further comprising the step of alerting an operator in case the verifying step results in the discovery of one or more non-authentic random number - sequence number pairs.

18. A method according to any of claims 1-17, wherein the step of generating a random number is performed upon the request from a user.

19. A method according to any of claims 1-18, further comprising the step of receiving payment from a user.

20. A method according to any of claims 1-19, wherein the verifying step comprises checking that a certain number of random numbers has been generated.

21. A method according to any of claims 1-20, wherein the verifying step comprises the steps of:

- checking whether a given random number - sequence number pair has previously been stored in the storage means,
- marking said given random number - sequence number pair as a true pair in case it has previously been stored in the storage means, and
- alerting an operator in case the given random number - sequence number pair has not previously been stored in the storage means.

22. A secure and auditable on-line system comprising:

- a random number generator,
- means for providing a sequence number for each generated random number, so as to create a random number - sequence number pair,
- storage means for storing the created random number - sequence number pair,
- verifying means for verifying, at a chosen time, stored random number - sequence number pairs, so as to ensure that every stored random number - sequence number pair is an authentic random number - sequence number pair.

23. An on-line system according to claim 23, wherein the verifying means is adapted to perform verification at at least substantially equal time intervals.

24. An on-line system according to claim 23 or 24, wherein the random number generator is a true random number generator.

25. An on-line system according to any of claims 23-25, wherein the storage means has limited access.

26. An on-line system according to any of claims 23-26, wherein the random number generator has limited access.

27. An on-line system according to claim 26 or 27, wherein access to the limited access area(s) can only be obtained by one or more authorised persons.

28. An on-line system according to claim 28, wherein access to the limited access area(s) can only be obtained by two or more authorised persons.

29. An on-line system according to claim 29, wherein the two or more authorised persons each represents an authority, so that at least two authorities are represented when access to the limited access area(s) is obtained.

30. An on-line system according to claim 30, wherein at least one of the authorised persons represents an operator, and at least one of the authorised persons represents an auditor.

31. An on-line system according to any of claims 23-31, further comprising means for issuing a ticket comprising information relating to the sequence number.

32. An on-line system according to claim 32, wherein the on-line system is a lottery, and the issued ticket is a lottery ticket.

33. An on-line system according to claim 33, wherein the ticket further comprises information relating to a winning/no winning category of the ticket.

34. An on-line system according to claim 33 or 34, wherein the ticket is issued based upon the random number and a probability table, the on-line system further comprising means for updating the probability table in response to the issued ticket, so as to maintain an at least substantially fixed winning/no winning ratio.

35. An on-line system according to any of claims 23-32, wherein the on-line system is a code generation system.

36. An on-line system according to any of claims 23-32, wherein the on-line system is an encryption system.

37. An on-line system according to any of claims 23-32, wherein the on-line system is a money transfer system.

38. An on-line system according to any of claims 23-38, further comprising means for alerting an operator in case the verification results in the discovery of one or more non-authentic random number - sequence number pairs.

39. An on-line system according to any of claims 23-39, wherein the random number generator is adapted to provide a random number in response to a request from a user.

40 An on-line system according to any of claims 23-40, further comprising means for receiving payment from a user.

41. An on-line system according to any of claims 23-41, wherein the verifying means is adapted to checking that a certain number of random numbers has been generated.

42. An on-line system according to any of claims 23-42, wherein the verifying means further comprises:

- means for checking whether a given random number - sequence number pair has previously been stored in the storage means,
- means for marking said given random number - sequence number pair as a true pair in case it has previously been stored in the storage means, and
- means for alerting an operator in case the given random number - sequence number pair has not previously been stored in the storage means.

43. A device for providing security and audit ability in an on-line system, the device comprising:

- a random number generator,
- means for providing a sequence number for each generated random number, so as to create a random number - sequence number pair,
- storage means for storing the created random number - sequence number pair,
- verifying means for verifying, at a chosen time, stored random number - sequence number pairs, so as to ensure that every stored random number - sequence number pair is an authentic random number - sequence number pair,

the verifying means further comprising:

- means for checking whether a given random number - sequence number pair has previously been stored in the storage means,
- means for marking said given random number - sequence number pair as a true pair in case it has previously been stored in the storage means, and
- means for alerting an operator in case the given random number - sequence number pair has not previously been stored in the storage means,

wherein the storage means and the random number generator have limited access.

ABSTRACT

The present invention provides a method a system and a device for obtaining security and audit ability in an on-line system. The system is a closed system and only auditors and/or authorities have access to the system. By means of a random number generator and a processing means a random number - sequence number pair is generated and stored in a storage means. By verifying stored random number - sequence number pairs, every stored random number - sequence number pair can be authenticated.

Fig. 2

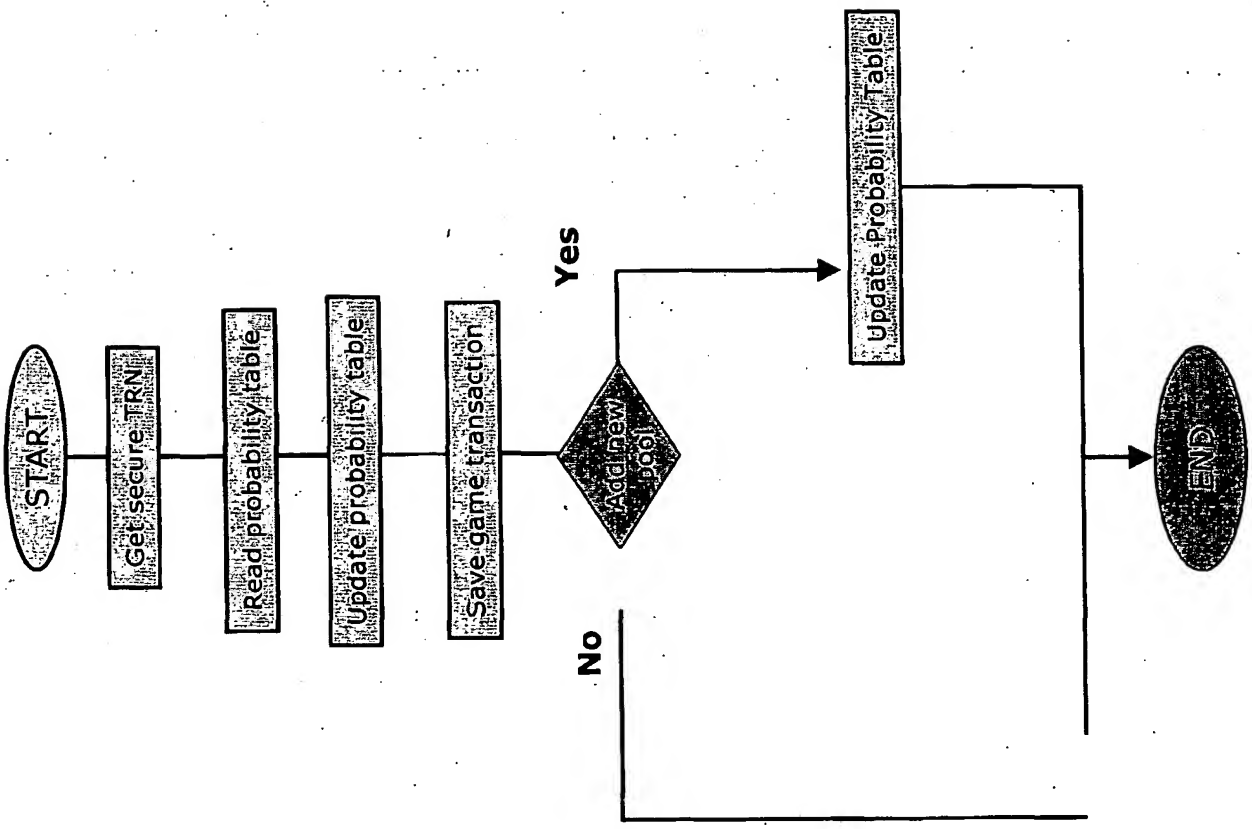
START
Get secure TRN
Read probability table
Update probability table
Save game transaction
Add new pool
Yes
No
Update Probability Table
END

Fig. 1

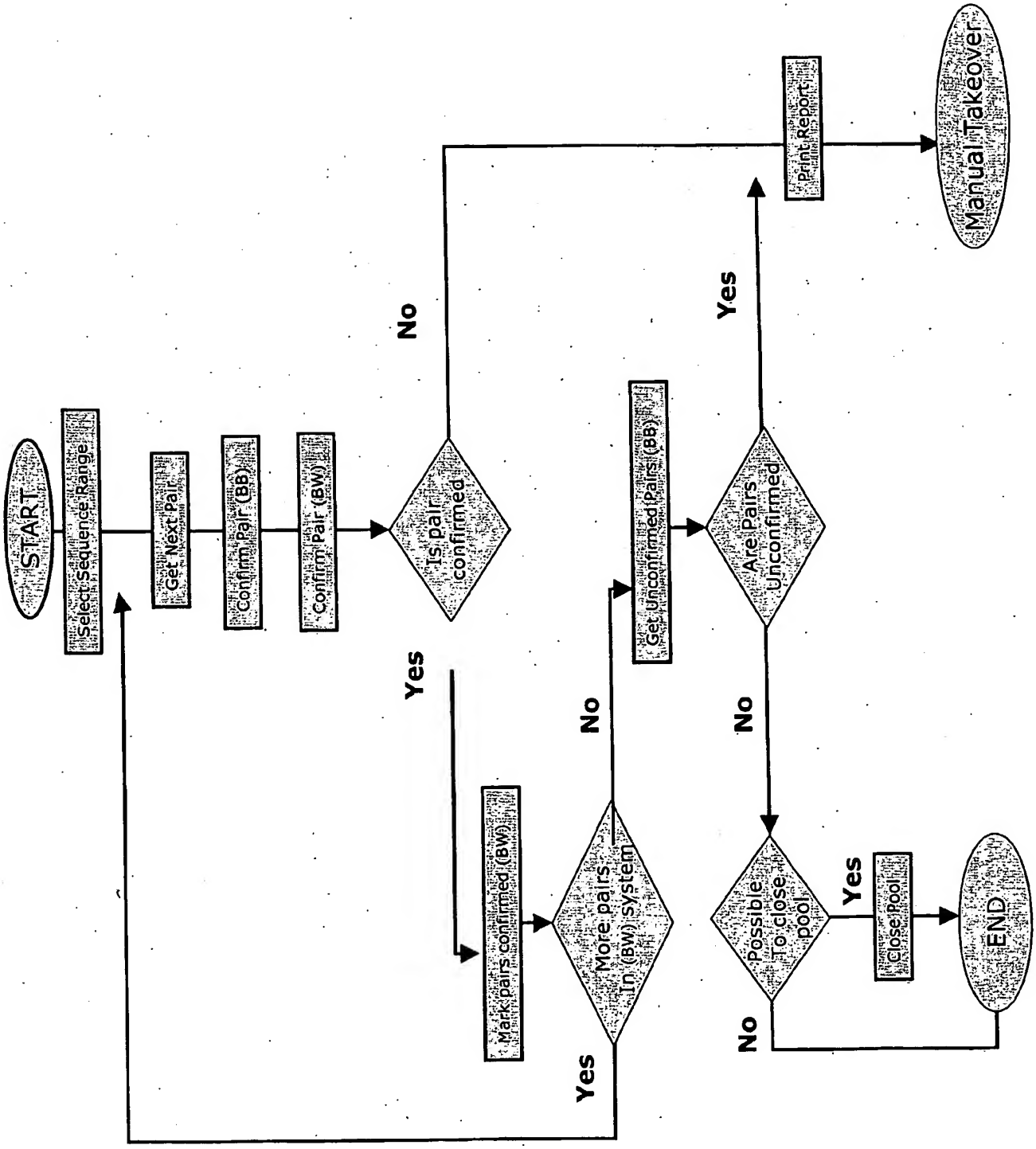
START
Select Sequence Range
Get Next Pair
Confirm Pair (BB)
Confirm Pair (BW)
Is pair confirmed
No
Print Report
Manual Takeover
Yes
Mark pairs confirmed (BW)
More pairs In (BW) system
No
Yes
Get Unconfirmed Pairs (BB)
Are Pairs Unconfirmed
Yes
No
Possible To close pool
Yes
Close Pool
END
No

Fig. 2

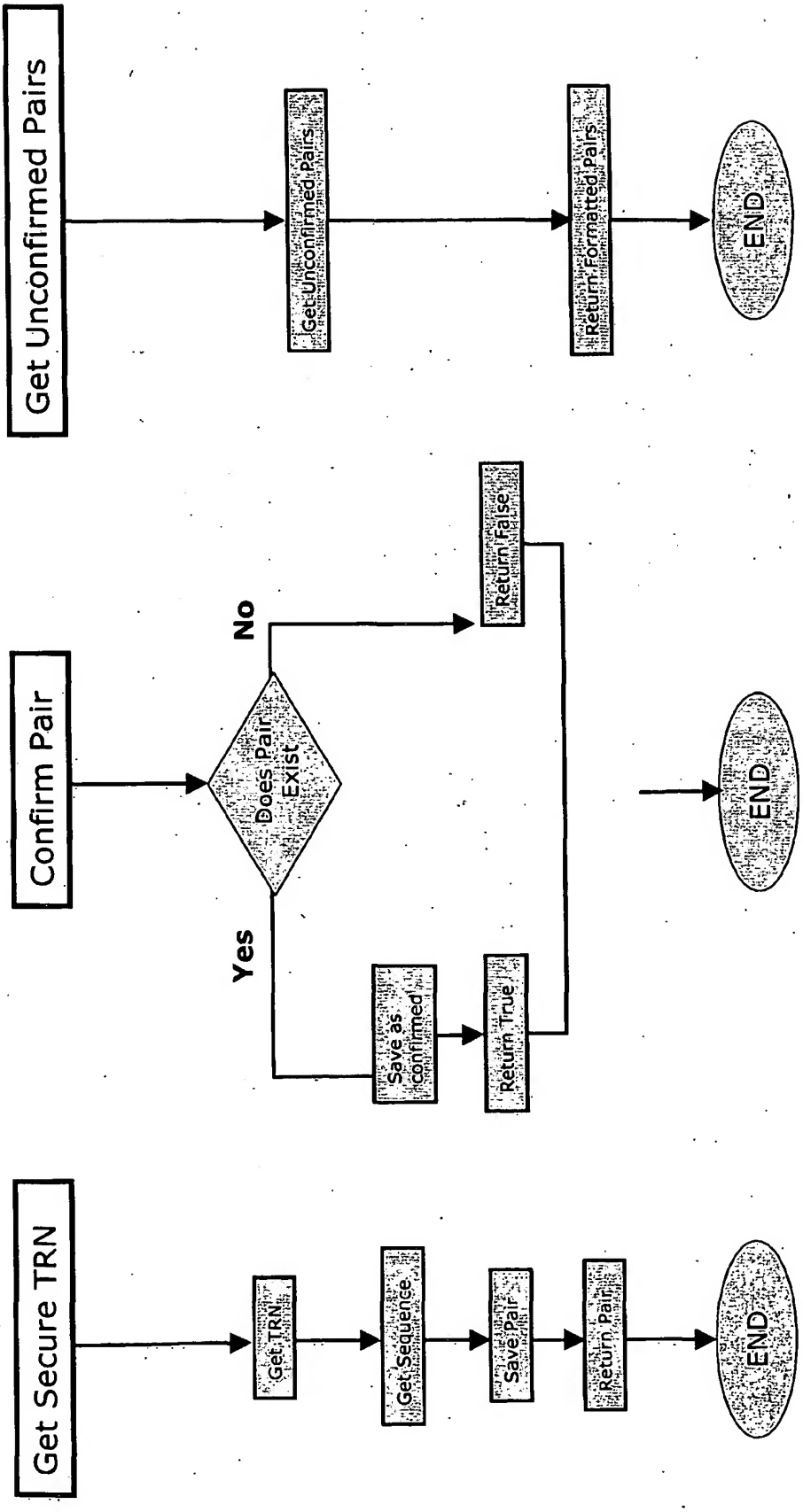
Get Unconfirmed Pairs
Get Unconfirmed Pairs
Return Formatted Pairs
END
Confirm Pair
Does Pair Exist
No
Return False
Yes
Save as confirmed
Return True
END
Get Secure TRN
Get TRN
Get Sequence
Save Pair
Return Pair
END

Fig. 3

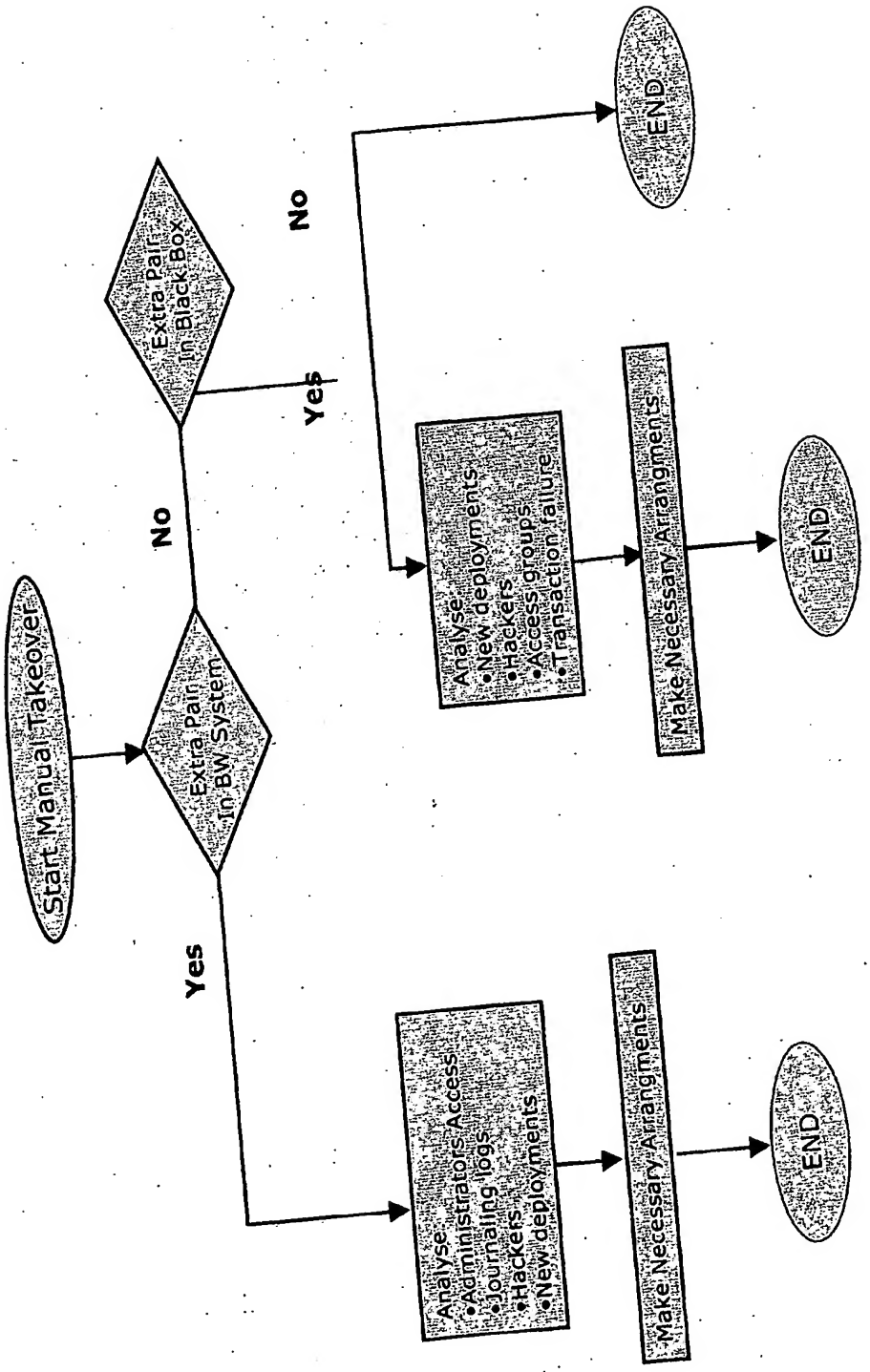
Start Manual Takeover
Extra Pair In BW System
No
Yes
Extra Pair In Black Box
No
Yes
END
Analyse
•New deployments
•Hackers
•Access groups
•Transaction failure
Make Necessary Arrangments
END
Analyse
•Administrators Access
•Journaling logs
•Hackers
•New deployments
Make Necessary Arrangments
END

Fig. 4